STEPHANIE M. HINDS (CABN 154284)
United States Attorney

THOMAS A. COLTHURST (CABN 99493)
Chief, Criminal Division

LAURA VARTAIN HORN (CABN 258485)
NICHOLAS WALSH (CABN 314290)
Assistant United States Attorneys

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-7200
Laura.Vartain@usdoj.gov
Nicholas.Walsh@usdoj.gov

NICHOLAS O. HUNTER (DCBN 1022355)
STEPHEN MARZEN (NYBN 2007094)
Trial Attorneys, National Security Division

950 Pennsylvania Ave., NW
Washington, DC 20530
Tel: (202) 353-3434
Fax: (202) 233-2146
Nicholas.Hunter@usdoj.gov
Stephen.Marzen@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. FUJIAN JINHUA INTEGRATED CIRCUIT CO., LTD, Defendant.	CASE NO. 18-CR-00465 MMC UNITED STATES' MOTION IN LIMINE TO AUTHENTICATE TWO SOLID STATES DRIVES ("SSDS") BY SOURCE AND EXPERT FORENSIC TESTIMONY ON THE CONTENTS OF THE DEVICES The Honorable Maxine M. Chesney Courtroom 7, 19th Floor

INTRODUCTION

Federal Rule of Evidence 901(b)(4) permits authentication of evidence by "appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances." Consistent with Rule 901(b)(4), the Ninth Circuit in *United States v. Matta-Ballesteros*, 71 F.3d 754, 768 (9th Cir. 1995), affirmed authentication of an audiotape based on the source of the audiotape ("the circumstances") and its contents. Four other Circuits have likewise upheld authentication of storage devices based on the source and contents of the devices, with at least one Circuit upholding authentication of a digital storage device (an iPhone) based entirely on the contents of the device, with no evidence of the source of the device.

In this case, the United States moves to authenticate forensic images of two solid state drives ("SSDs") based on their source (United Microelectronics Corporation ("UMC")) and their contents. The contents of the digital devices will be the subject of expert testimony by Andrew Crain, a computer forensic expert. Mr. Crain's testimony will tie each of the two solid state drives ("SSDs") used in J.T. Ho and Neil Lee's first UMC-issued laptops to the conspirators and establish when the devices were used by them. Rule 901(b)(4) permits the Court to consider Mr. Crain's expert testimony on the contents of the digital storage devices in order to determine that those devices are authentic. During Mr. Crain's testimony, the government will move in evidence the two SSDs and Federal Rule of Evidence 1006 summary exhibits of the relevant information contained on the two SSDs.

THE DIGITAL STORAGE DEVICES AT ISSUE

The United States seeks authentication of two SSDs, designated as devices 27 and 28. Neither of these two SSDs was seized by the Taiwanese Ministry of Justice Investigation Bureau ("MJIB"). Instead, the United States Federal Bureau of Investigation ("FBI") obtained each drive from FRONTEO, a storage and forensic analysis company, who had in turn obtained the drives directly from UMC. The Court heard testimony about that chain of custody from FRONTEO representative Patrick Newton and received two exhibits documenting that exchange. *See* P1519 and P1520 (together establishing that UMC gave the two SSDs to FRONTEO on March 20, 2020, and that the two SSDs were given to the FBI on April 12, 2021). Exhibit P1519 further establishes, by way of photograph, that the two SSDs

were: (a) one portable Intel SSD 535 Series, 240GB, ISN: CVTR539306K0240CGN, accompanied by a yellow note with handwritten Chinese characters and in English "Neil Lee" (device 27) and (b) one portable Intel SSD 535 Series, 240GB, ISN: CVTR542105VZ240CGN, accompanied by a yellow note with handwritten Chinese characters and in English "JT Ho" (device 28). Exhibit 1520 further establishes that those same devices were released on April 12, 2021 (by recording the two SSD serial numbers).

Further, by stipulation of the parties, it is established that:

8) On or about April 12, 2021, a United States FBI Special Agent personally obtained from a representative at FRONTEO Taiwan, Inc., in Taipei City, Taiwan:

a) One sealed envelope with label containing Chinese characters and "FRONTEO Taiwan, Inc. FTW-000157 4/8/2021 TUH193." Inside the envelope wrapped in the plastic was: (a) one portable Intel SSD 535 Series, 240GB, ISN: CVTR539306K0240CGN; (b) a yellow note with handwritten Chinese characters and in English "Neil Lee" and (c) a white FRONTEO Taiwan, Inc. label marked "Case No. T1806052; Location: UMC Hsinchu; Date:(M/D/Y) 3/20/2020; Evidence No./Memo: TUHI93;" and

b) One sealed envelope with label containing Chinese characters and "FRONTEO Taiwan, Inc. FTW-000158 4/8/2021 TUH194." Inside the envelope wrapped in the plastic was: (a) one portable Intel SSD 535 Series, 240GB, ISN: CVTR542105VZ240CGN; (b) a yellow note with handwritten Chinese characters and in English "JT Ho" and (c) a white FRONTEO Taiwan, Inc. label marked "Case No. T1806052; Location: UMC Hsinchu; Date:(M/D/Y) 3/20/2020; Evidence No./Memo TUH194."

9) The items described in paragraphs 8(a) and 8(b) were brought to the United States and were in continuous United States FBI custody until United States FBI Special Agent Cynthia Ho personally delivered the items to Matthew Moore, Associate

Director at Berkeley Research Group, LLC, in Palo Alto, California, on April 30, 2021.

10) The items described in paragraphs 8(a) and 8(b) were in continuous custody of Berkeley Research Group, LLC, between April 30, 2021, and August 30, 2021.

11) Matthew Moore, Associate Director at Berkeley Research Group, LLC, personally returned the items described in paragraphs 8(a) and 8(b) directly to United States FBI Special Agent Cynthia Ho in Palo Alto, California, on August 30, 2021.

12) The items described in paragraphs 8(a) and 8(b) have remained in continuous United States FBI custody since August 30, 2021.

The United States' computer forensic expert, Mr. Crain, works at Berkeley Research Group, LLC. As the testimony will establish, it was during Berkeley Research Group, LLC's custody of the two devices that images were made and analysis was performed.

The forensic evidence of the two Intel SSD 535 Series, 240GB, SSDs will establish that one SSD was used by J.T. Ho[1] and the other by Neil Lee[2] in the first weeks of their employment at UMC. Mr. Crain will explain precisely what evidence ties to J.T. Ho and Neil Lee. One SSD shows Neil Lee's UMC User Profile. The other SSD shows J.T. Ho's UMC User Profile. Forensic analysis will further demonstrate precisely when the SSDs were in use, which was mid-November through December 4, 2015. Relatedly, the Court heard testimony from UMC employees J.C. Cho and C.S. Chang that also on December 4, 2015, there was both an unusual request to reformat two hard drives as well as a request for replacement SSDs from the same department and floors that J.T. Ho and Neil Lee worked on in FAB12A in Tainan Science Park. *See* P1151.0002 (request for new Intel SSD 535 Series, 240GB 2.5" SSD from the 6th Floor of FAB 12A (the same floor J.T. Ho's new computer application states in

[1] Documents establishing the issuance of J.T. Ho's UMC laptop on or after November 6, 2015, were admitted as P1075T.0003 to 0007, and contain the same specific type of SSD the government seeks to admit: an Intel SSD 535 Series, 240GB SSD. *See also* P1190T.0001 (tying J.T. Ho to UMC computer 035481).

[2] Documents establishing the issuance of Neil Lee's UMC laptop on or after November 24, 2015, were admitted as P1075T.0009 to 0011, and contain the same specific type of hard drive the government seeks to admit: an Intel SSD 535 Series, 240GB SSD. *See also* P1191T.0001 (tying Neil Lee to UMC computer 035551).

P1075T.003)); P1147T (request for new Intel SSD 535 Series, 240GB 2.5" SSD from the 9th Floor of FAB 12A (the same floor Neil Lee's new computer application states in P1075T.003)). UMC documents in evidence establish that J.T. Ho's employee number at UMC was 00046294 and Neil Lee's was 00046324. *See* P1190T.0001 (J.T. Ho); P1075T.0009 (Neil Lee); and P119T.0001 (Neil Lee). Mr. Crain's analysis identifies those profiles on the SSDs.

As explained below, this evidence is more than sufficient to authenticate and, in the end, admit the two SSDs and Federal Rule of Evidence 1006 summary exhibits of the relevant information contained on the two SSDs in evidence.

ARGUMENT: THE COURT CAN AUTHENTICATE THE FORENSIC IMAGES OF THE TWO SSDS BASED ON SOURCE AND CONTENT ALONE

A. Authentication Requires Only a *Prima Facie* Case

Evidence is "authentic" if there is "evidence sufficient to support a finding that the item is what the proponent claims it is." FED. R. EVID. 901(a). To authenticate evidence under Rule 901, "[t]he government need only make a *prima facie* showing of authenticity, as '[t]he rule requires only that the court admit evidence if sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity or identification.'" *United States v. Tank*, 200 F.3d 627, 630 (9th Cir. 2000) (citations omitted).

"[A] defect in the chain of custody goes to the weight, not the admissibility, of the evidence introduced." *United States v. Matta-Ballesteros*, 71 F.3d 754, 769 (9th Cir. 1995). Indeed, chain-of-custody evidence "is merely one possible means of authentication and not . . . an exclusive requirement." *United States v. Browne*, 834 F.3d 403, 411–15 (3d Cir. 2016); *see United States v. Camuti*, 78 F.3d 738, 743 (1st Cir. 1996) ("Chain of custody is one means of authenticating evidence but not the only means . . . ."). Rather, "proponents of exhibits may also prove their authenticity with circumstantial evidence." *United States v. Crosgrove*, 637 F.3d 646, 658 (6th Cir. 2011) (quoting 1-8 Weinstein's Evidence Manual § 8.01).

B. The Ninth Circuit and Four Other Circuits Authenticate Storage Devices Based on Source and Contents

In *Matta-Ballesteros*, 71 F.3d 754, the Ninth Circuit upheld the district court's authentication of an audiotape of the torture of a DEA agent that was found in the torture house (*id*. at 761) and based on identification of the speakers heard on the tape (*id*. at 768). The Court held that the audiotape was what the government purported it to be – an audio recording of the torture of the DEA agent – based solely on the source and contents of the tape, even though the government had no chain of custody from the time the tape was recorded until the tape came into the government's possession. *Matta-Ballesteros* is binding authority for the proposition that source and contents alone can authenticate storage devices.

Four other circuits similarly uphold authentication of digital storage devices based on source and content. One circuit – the Fourth – upheld authentication of a digital storage devices based on the contents of the device alone. In *United States v. Reed*, 780 F.3d 260, 269 (4th Cir. 2015), the Fourth Circuit held that "the government could still connect the phone to Dyer based on its data, namely its stored photos and text messages, which demonstrated that he owned and possessed the phone." "[A]t trial, the government offered no testimony about how this phone was seized." *Id*. at 265. The Fourth Circuit nonetheless upheld the district court's authenticity determination because there was evidence of "photos of Dyer on the phone and text messages attributing the number to Dyer, including several that used variations on his first name." *Id*. at 267.

In *United States v. Lewisbey*, 843 F.3d 653, 658 (7th Cir. 2016), the Seventh Circuit upheld the district court's authentication of text messages from two cell phones based on the source and contents of the cellphones. An iPhone was authenticated because it was "confiscated from Lewisbey" and Lewisbey told his mother that police took his phone. *Id*. A Samsung phone was authenticated because it was "recovered from his bedroom" and the Properties and Contacts directories tied the device to Lewisbey. *Id*. Both cell phones also listed contact information for a former employer. *See id*. According to the Seventh Circuit, "[t]hat's more than enough to establish that the two phones were indeed Lewisbey's."

In *United States v. Siddiqui*, 235 F.3d 1318, 1322–23 (11th Cir. 2000), the Eleventh Circuit affirmed authentication of e-mail messages based on the address, contents, substance of the message, and use of the author's nickname. *See also United States v. Fluker*, 698 F.3d 988, 999-1000 (7th Cir.

2012) (authenticating e-mail message as from defendant based on address, author, and content).

Lastly, in *United States v. Browne*, 834 F.3d 403, 413-14 (3d Cir. 2016), the Third Circuit affirmed authentication of FaceBook records of online conversations between a defendant and minors (among other participants) based on content, defendant's admission of a link to the FB account, personal account information consistent with the defendant's personal information, and FB's recording of posts through the company's electronic systems.

The Circuit Courts of Appeal that have addressed the issue have all upheld the authentication of storage devices based on the source and contents of the devices without more.

Federal Rule of Evidence 901(b)(4) premises authentication not only on source, contents, and other distinctive characteristics, but also takes into account "all the circumstances." In determining authenticity, Rule 901(b)(4) allows the Court to consider the totality of the circumstances. Mutually reinforcing circumstances may suffice to make a *prima facie* case that the device is what the government purports it to be even if the contents of the devices considered in isolation would not. That one item in a particular location is determined to be *prima facie* authentic, helps authenticate the other items located in the same location or another location associated with the same defendant. For example, once one enters a bedroom and finds several items (*e.g.*, an addressed envelope, a cellphone, and bill) associated with one person, that fact tends to establish that the other items in the bedroom are also associated with that person – even if the items cannot otherwise be directly tied to the person (*e.g.*, because they are non-descript items such as illegal narcotics or an unregistered firearm). *See United States v. Gonzales*, 307 F.3d 906, 910 (9th Cir. 2002) ("In the present case, the pay/owe sheets were found in the backpack with the gun, drugs, scale and other drug paraphernalia which 'circumstantially authenticated' the sheets, making their relevance as evidence of drug distribution clear.").

C. Because Digital Storage Devices may be Authenticated Based on Their Content, the Court may Hear Expert Forensic Testimony of the Forensic Images of the Two SSDs Before Those Images are Admitted into Evidence

Rule 901(b)(4) permits evidence such as digital storage devices to be authenticated based on their "contents." The evidence rules also permit the Court to hear expert evidence on matters outside the ken of lay witnesses. *See, e.g.*, Fed. R. Evid. 904(b)(3) (permitting comparison by and "expert witness" to authenticate a specimen). To avoid the Catch-22 between the need for expert forensic testimony in

order to see the contents of the two SSDs, on the one hand, and the preclusion of expert testimony on images that have not been admitted into evidence, it would seem sensible to permit the forensic expert to testify to the contents of the two SSDs in order to authenticate and admit them in evidence.

CONCLUSION

The Court should permit forensic expert Mr. Crain to testify about the contents of the forensic images of the two SSDs numbered 27 and 28 before those devices are admitted into evidence and consider that expert testimony in determining the admissibility of those devices.

During Mr. Crain's testimony, the government will move the forensic images of the digital storage devices into evidence along with the forensic images of the stipulated devices, which Mr. Crain would then analyze and present in part through Federal Rule of Evidence 1006 summary exhibits.

Dated: March 9, 2022

Respectfully Submitted,

STEPHANIE M. HINDS
United States Attorney

/s/
LAURA VARTAIN HORN
NICHOLAS WALSH
Assistant United States Attorneys

NICHOLAS O. HUNTER
STEPHEN MARZEN
Trial Attorneys, National Security Division